REMARKS

This Amendment and the following remarks are intended to fully respond to the Office Action mailed September 2, 2008, hereinafter "Office Action." In the Office Action, claims 1-9, 18-22, 26, and 27 were examined and all claims were rejected. More specifically, claims 1-6, 8-9, 18-21, and 26-27 were rejected under 35 U.S.C. § 102(b) as being allegedly anticipated by "Further Analysis of the Internet Key Exchange Protocol," H. Zhou, Computer Communications, Vol. 23, Issue 17, pp. 1606-1612, 2000, hereinafter "Zhou"; and claims 7 and 22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Zhou in view of Inoue et al. (USPN 6,170,057), hereinafter "Inoue".

In this Amendment, claims 1, 18, 26, and 27 been amended and no claims have been cancelled or added. Therefore, claims 1-9, 18-22, and 26-27 remain present for examination.

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested.

Claim Rejections under 35 U.S.C. 102

Claims 1-6, 8-9, 18-21, and 26-27 were rejected under 35 USC § 102(b) as being anticipated by Zhou. Applicants respectfully traverse the § 102(b) rejections because either the Office Action has failed to state a prima facie case of anticipation or the current amendments to the claims now renders the Office Action's arguments moot. A *prima facie* case of anticipation can be met only where the reference teaches each and every aspect of the claims. *See* MPEP §§ 706.02 & 2133. Under 35 U.S.C. § 102, a reference must show or describe each and every element claimed in order to anticipate the claims. *Verdegaal Bros. v. Union Oil Co. of California* 814 F.2d 628 (Fed. Cir. 1987) ("A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference"). More specifically, the reference fails to teach or suggest, *inter alia*, wherein a message is exchanged between the responder and the initiator before the completion of the IKE main mode negotiation, the message comprising at least part of the IKE quick mode negotiation, and the message including both a main mode pseudo random number and a separate quick mode pseudo random number, as recited in independent claim 1.

Zhou is an examination of some security issues in regard to the Internet Key Exchange (IKE) protocol specified in RFC 2409. (*See* Zhou, Abstract). Zhou provides an overview of the IKE protocol. According to the reference, the IKE protocol is designed to exchange keying material and negotiate security associations for secure communication. The protocol works in two phases. Phase 1 establishes an ISAKMP SA and derives shared secrets *that will be used to protect Phase 2 exchanges*. Phase 2 negotiates SAs for IPSEC and generates fresh keying materials. According to the reference, the IKE protocol defines three basic modes of exchanges including a *main mode* that is **used in Phase 1** and a *quick mode* that is **used in Phase 2**. (*See* Zhou, p. 1606, §2). The reference provides a detailed discussion of the main mode describing the six exchanges between an initiator and a responder in the main mode protocol. (*See* Zhou, p. 1607, §2.2). Zhou additional provides a discussion of the three exchanges involved in the quick mode protocol. (*See* Zhou, p. 1607, §2.2).

While Zhou provides a discussion of the main mode and quick mode phases of the IKE protocol, the reference fails to teach or suggest wherein a message is exchanged between the responder and the initiator before the completion of the IKE main mode negotiation, the message comprising at least part of the IKE quick mode negotiation, and the message including both a main mode pseudo random number and a separate quick mode pseudo random number. The Office Action argues that the Zhou's description of the IKE main mode and IKE quick mode as teaching wherein at least one message that comprises at least part of the IKE quick mode negotiation is sent during the IKE main mode negotiation and a quick mode pseudo random number is exchanged between the responder and the initiator before completion of the IKE main mode negotiation, as previously recited in independent claim 1. However, Zhou merely describes the steps of IKE quick mode and IKE main mode. Indeed, the reference describes main mode occurring during Phase 1 of the IKE protocol and quick mode occurring during Phase 2 of the protocol. (*See* Zhou, p. 1606, §2, "*main mode* and *aggressive mode* used in Phase 1, and quick mode used in Phase 2"). Moreover, as described Phase 1 must necessarily occur before Phase 2 because "Phase 1 establishes an ISAKMP SA and *derives shared secrets that will be used to protect Phase 2 exchanges*." (Zhou, p. 1606, §2) (emphasis added). This is the standard way of practicing the IKE protocol.

On the other hand, the claimed embodiments are not directed to practicing the IKE protocol as described in Zhou and detailed in RFC 2409. Instead, the claimed embodiments are directed to a more efficient way of practicing internet key exchange. To that end, in claim 1 a message is exchanged between the responder and the initiator before the completion of the IKE main mode negotiation, the message comprising at least part of the IKE quick mode negotiation, and the message including both a main mode pseudo random number and a separate quick mode pseudo random number. Because Zhou is directed towards regular IKE protocol exchanges, the reference fails to teach at least: the message includes a main mode pseudo random number and a quick mode pseudo random number. Instead, the reference clearly teaches a two phased approach; phase 1 conducting main mode negotiations *followed by* a second phase in which the quick mode negotiation takes place.

The Office Action argues that because the variable N_r appears in both the fourth exchange of main mode negotiation and the second exchange of the quick mode negotiation described in Zhou, "N_r can be interpreted as a part of the IKE quick mode negotiation." Applicants respectfully disagree. Indeed, N_r is merely a variable representing a type of payload during the main mode and quick mode negotiations. Even if N_r could be considered the same variable in both negotiations described in the Zhou reference (and Applicants respectfully submit that it cannot), the fact that N_r appears in both negotiations does not teach a message is exchanged between the responder and the initiator before the completion of the IKE main mode negotiation, the message comprising at least part of the IKE quick mode negotiation, and the message including both a main mode pseudo random number and a separate quick mode pseudo random number. For at least the forgoing reasons, independent claim 1 is allowable over the cited reference.

For at least similar reasons, independent claim 18 is also allowable over the cited reference. Independent claim 18 recites, *inter alia*, wherein a message is exchanged between the responder and the initiator before completion of the IKE main mode negotiation, the message comprising at least part of the IKE quick mode negotiation, and the message including both a main mode pseudo random number and a separate quick mode pseudo random number.

Additionally, independent claim 26 is also allowable over the cited reference for at least similar reasons. Independent claim 26 recites, *inter alia*, receiving, at the initiator, a second message, wherein the second message comprises at least part of the IKE main mode negotiation and at least part of an internet key management and exchange protocol (IKE) quick mode negotiation and the IKE quick mode negotiation comprises deriving a set of keys usable with the security protocol and wherein the second message includes both a main mode pseudo random number and a separate quick mode pseudo random number.

Finally, independent claim 27 is also allowable over the cited reference for at least similar reasons as discussed with respect to claim 1. Claim 27 recites, *inter alia*, sending, from the responder, a second message, wherein the second message comprises at least part of the IKE main mode negotiation and at least part of an internet key management and exchange protocol (IKE) quick mode negotiation and wherein the IKE quick mode negotiation comprises deriving a set of keys usable with the security protocol and wherein the second message includes both a main mode pseudo random number and a separate quick mode pseudo random number.

For at least the foregoing reasons, independent claims 1, 18, and 26-27 are allowable over the cited reference. All other claims, *i.e.*, claims 2-9, and 19-22 depend from the allowable independent claim and are, thus, also allowable over the cited references. Therefore, Applicants respectfully request that the Examiner issue a notice of allowance, for all claims, at the Examiner's earliest convenience.

Claims Rejections under 35 U.S.C. §103

Claims 7 and 22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Zhou in view of Inoue. Claims 7 and 22 depend from claims 1 and 18 respectively. Thus, claims 7 and 22 are also allowable by virtue of their dependence off of allowable independent claims 1 and 18. Inoue does not make up for the deficiencies of Zhou. Applicants therefore respectfully request that the Examiner withdraw the rejection and issue a notice of allowance for all claims.

CONCLUSION

This Amendment fully responds to the Office Action mailed on September 2, 2008. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicants believe the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the art of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

It is believed that no further fees are due with this Amendment. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance, and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is respectfully requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: January 2, 2009

Gregory D. Leibold, Reg. No. 36,408
Merchant & Gould P.C.
PO Box 2903
Minneapolis, MN 55402-0903
303.357.1642